



Incorrect boundary conditions in the Networking: JAR component

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-2779 |
| State | PUBLISHED |
| Assigner | mozilla |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-02-24 14:16:26 UTC |
| Updated | 2026-04-13 15:17:25 UTC |
| Description | Incorrect boundary conditions in the Networking: JAR component. This vulnerability was fixed in Firefox 148, Firefox ESR 1 |

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000650000 probability, percentile 0.201070000 (date 2026-04-15)

Problem Types: NVD-CWE-noinfo | CWE-119 | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | ADP | DECLARED | 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------|-------------|---------|--------|---------|----------|
| Application | Mozilla | Firefox | All | All | All | All |
| Application | Mozilla | Firefox | All | All | All | All |
| Application | Mozilla | Thunderbird | All | All | All | All |
| Application | Mozilla | Thunderbird | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---------|-------------|----------------------------|---------------|
| CNA | Mozilla | Firefox | unaffected 140.8 140.* rpm | Not specified |
| CNA | Mozilla | Firefox | unaffected 148 * rpm | Not specified |
| CNA | Mozilla | Thunderbird | unaffected 140.8 140.* rpm | Not specified |
| CNA | Mozilla | Thunderbird | unaffected 148 * rpm | Not specified |

References

| Reference | Source | Link | Tags |
|--|----------------------|--|--------------------------------------|
| www.mozilla.org/security/advisories/mfsa2026-13 | security@mozilla.org | www.mozilla.org | Vendor Advisory |
| www.mozilla.org/security/advisories/mfsa2026-17 | security@mozilla.org | www.mozilla.org | Vendor Advisory |
| www.mozilla.org/security/advisories/mfsa2026-16 | security@mozilla.org | www.mozilla.org | Vendor Advisory |
| www.mozilla.org/security/advisories/mfsa2026-15 | security@mozilla.org | www.mozilla.org | Vendor Advisory |
| bugzilla.mozilla.org/show_bug.cgi | security@mozilla.org | bugzilla.mozilla.org | Issue Tracking, Permissions Required |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

CNA: Alex Mayorga (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)